UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,	)	
Plaintiff,	)	
v.	)	**Criminal No. 09-40021-FDS**
DAVID LADEAU,	)	
Defendant.	)	

MEMORANDUM AND ORDER
ON DEFENDANT'S MOTION TO SUPPRESS

SAYLOR, J.

This is a prosecution for possession of child pornography. Defendant David Ladeau has moved to suppress various items of evidence that were seized at his apartment as a result of a search. Relying on information obtained from Canadian police authorities, American federal law enforcement agents obtained a warrant to search Ladeau's apartment on April 14, 2009. Federal agents executed the search warrant on April 15, 2009. They seized, among other items, a computer and several digital storage devices, including CDs and DVDs. Ladeau was indicted on June 16, 2009, on one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(b).

On February 12, 2010, Ladeau filed a motion to suppress all of the evidence seized as a result of the search of his apartment. Ladeau contends that a warrantless search of his computer was conducted in violation of the Fourth Amendment; that the information contained in the affidavit supporting the warrant was stale at the time the warrant was obtained; and that the

agents failed to review the material they seized within the time period required by law.

For the reasons set forth below, the motion to suppress will be denied.

I. Background

In November 2007, the Royal Canadian Mounted Police ("RCMP") in Winnipeg, Manitoba, arrested an individual for child exploitation offenses. The individual had used Gigatribe software on his computer to post several videos depicting child pornography onto an online network for exchange. After the arrest, the RCMP, with the individual's consent, began using the individual's online identity to engage with other potential suspects. These suspects included people within the individual's Gigatribe network. (April 14, 2009 LaForte Aff. ¶ 16).

Gigatribe is a peer-to-peer file-sharing program that allows users to share computer files with other users in their network. The Gigatribe software enables a user to create his own private network, which he controls. He can invite guests to join his network, and remove guests from his network at any time. He can also prevent other users from viewing his personal information without his permission. A user can also join the networks of other Gigatribe users, but only with the permission of the user who created the network. Users select specific folders on their computers they wish to share with other users in the network. These folders may contain video, audio, or image files. A guest accepted to join a network can access any files that have been selected to be shared. (*Id*. ¶ 10).

Users have the ability to search for specific files located on other users' computers. They can scroll through the available files to choose which files to download. The files may be available in thumbnail format, which provides a preview to anyone considering whether to download the files. (*Id*. ¶ 11). Gigatribe software encrypts files before transmitting them from

one user to another. Once received, the file is then decrypted to allow the user to view it. (*Id*. ¶ 13). Gigatribe also features a chat function that allows user to communicate with each other via computer. (*Id*. ¶ 14). Gigatribe places no limit on the size of files that can be exchanged. This means one user can transmit several video files at a time to another user. (*Id*. ¶ 15).

The undercover investigation using the arrested individual's online identity began on November 23, 2007. On August 20, 2008, an undercover investigator downloaded 171 files believed to be child pornography. These files were designated for sharing through Gigatribe by a user called "Tjayxx." Three of the files contained videos of pre-pubescent boys and girls engaged in sex acts with other pre-pubescent children and adult men. (*Id*. ¶ 18).

Gigatribe records showed that user "Tjayxx" signed onto Gigatribe on August 24, 2008, using IP address 216.195.19.156. According to the same records, "Tjayxx's" last log-on before the warrant was obtained was on October 15, 2008, from the same IP address. Gigatribe records contained two e-mail addresses for "Tjayxx": Tjay@hushmail.com and dladeau@townisp.com. (Id. ¶ 19).

On April 2, 2009, Eric LaForte, a special agent with the Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), was informed by Gigatribe officials that it is not possible to have two accounts with the same username on the Gigatribe network. It is also not possible to run the same Gigatribe account on two computers at the same time. LaForte concluded, therefore, that when the undercover investigator downloaded the files on August 20, 2008, there was only one user on Gigatribe named "Tjayxx." (Id. ¶ 20).

Further investigation by LaForte revealed that IP address 216.195.19.156 is provided by Shrewsbury Electric and Cable Operations ("SELCO"). To determine the identity of the user of

the IP address on August 24, 2008, and October 15, 2008, ICE issued an administrative subpoena to SELCO on February 23, 2009. In response, SELCO identified David Ladeau of Shrewsbury, MA, as the user of the IP address on those dates. As of February 23, 2009, Ladeau's account was listed as "active" and he had an e-mail address of dladeau@townisp.com. That e-mail address was one of the addresses listed on the "Tjayxx" Gigatribe account. (Id. ¶ 21). LaForte contacted SELCO on April 2, 2009, which informed him that Ladeau utilized IP address 216.195.19.156 from July 14, 2008, through October 23, 2008, continuously. (Id. ¶ 22).

The Massachusetts Registry of Motor Vehicles databases revealed that David Ladeau is a resident of Shrewsbury. LaForte visited the address listed in the RMV registry and saw Ladeau's name on a mailbox located at the residence. After speaking with a detective from the Shrewsbury Police Department, LaForte determined that Ladeau lived alone at the address contained in the RMV database. (Id. ¶ 23).

LaForte's investigation also revealed that on October 24, 2008, Ladeau was charged in the Westborough District Court with two counts of indecent assault and battery on a child, two counts of showing obscene material to a minor, and one count of enticing a child under the age of 16. All of those counts remained pending in the Westborough District Court at the time the warrant was obtained. (Id. ¶ 24). LaForte then spoke with Detective Randolph Holmquist of the Shrewsbury Police Department and reviewed material related to the investigation of the case. LaForte learned that Ladeau was accused of taking at 12-year-old boy to an adult video store near Ladeau's home on or about July 6, 2008. Ladeau then brought the boy back to Ladeau's home, where he showed him pornography and molested him. The alleged victim eventually insisted that Ladeau drive him home, and Ladeau complied. (Id. ¶ 25).

On April 14, 2009, LaForte submitted an affidavit in support of the application for a warrant to search Ladeau's apartment. He recited, among other things, all of the facts outlined above. He also included observations from knowledge he had gained by performing investigations into cases involving child pornography and computer crimes. He stated that individuals who have a sexual interest in children and who share and distribute child pornography "are often child pornography collectors who have escalated their activity from anonymously obtaining free images of child pornography on the Internet to proactively distributing images they have collected . . . ." (Id. ¶ 26). He went on to state that such collectors almost always maintain hard copies of their collections, often for many years. (Id. ¶ 27(C)). He stated that based on his investigation into the case, there was probable cause to believe Ladeau is a collector of child pornography with a sexual interest in children. (Id. ¶ 28).

In the affidavit, LaForte described the extensive amount of time it takes to analyze computer evidence. Computer storage devices can store vast amounts of data. The majority of computers sold today can store the equivalent of about ten million typewritten double spaced pages of text. This data is often concealed by being stored in random order with deceptive file names. Sifting through all this data and analyzing it can take days or even weeks and must be done in a controlled environment. (Id. ¶ 31,34).

The magistrate issued the warrant on April 14, 2009. It was ordered to be returned by April 24, 2009. The search was conducted on April 15, 2009, and several items, including computer equipment and various digital storage devices, were seized. The examination of all of the items seized was completed on May 13, 2009.

II. Analysis

Defendant advances three arguments as to why the evidence seized pursuant to the search warrant should be suppressed. First, he contends that the remote download of files from his computer by the RCMP was a warrantless search in violation of the Fourth Amendment. Second, he contends that there was no probable cause to conclude that child pornography would be found at his apartment eight months after the initial images were downloaded from his computer. Third, he contends that law enforcement officials failed to examine the digital media seized from the defendant's home within the time frame prescribed by law. The Court will address each of these arguments in turn.

A. The Remote Download of Files from Ladeau's Computer

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." U.S. Const. amend. IV. The Fourth Amendment generally protects privacy interests where an individual has a reasonable expectation of privacy. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). The United States Supreme Court established a two-part test to determine when an individual has a reasonable expectation of privacy: the individual must have (1) a subjective (or actual) expectation of privacy, and (2) such an expectation must be one that "society is prepared to recognize as reasonable." *Id*. (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

Ladeau contends that he had a reasonable expectation of privacy in the files the RCMP downloaded from his computer. Specifically, he argues that by using Gigatribe software, which contains several features that are designed to prevent members of the general public from

accessing his computer files, he exhibited a subjective expectation of privacy. He also contends that because society has increasingly come to rely on the Internet to complete many transactions that require a measure of privacy (such as banking, shopping, corresponding through e-mail, and the like), society is prepared to recognize an expectation of privacy on a peer-to-peer network (such as Gigatribe) as reasonable.

The government contends that while Ladeau may have had a subjective expectation of privacy, any such expectation was not objectively reasonable. According to the government, regardless of the amount of privacy safeguards Gigatribe offers its users, an individual cannot have a reasonable expectation of privacy in information he voluntarily shares with another person.

Several courts have held that users of peer-to-peer software, such as LimeWire, do not have an objectively reasonable expectation of privacy in the contents of the computer they use to run the software. See *United States v. Stults*, 575 F.3d 834, 842-843 (8th Cir. 2009); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Brese*, No. CR-08-52-D, 2008 WL 1376269, at *2 (W.D. Okla. April 9, 2008). In *Ganoe*, the Ninth Circuit noted that anyone who installs and uses file-sharing software is "opening his computer to anyone else with the same freely available program." A person who grants the public access to his computer cannot be said to have an objectively reasonable expectation of privacy in that computer. *Ganoe*, 538 F.3d at 1127.

Ladeau contends that while LimeWire users may not have a reasonable expectation of privacy in the contents of their computers, the same cannot be said of Gigatribe users. That is because Gigatribe contains safeguards to prevent unauthorized users from accessing a Gigatribe

user's computer. As Agent LaForte described in his affidavit in support of the warrant, an individual may only access a Gigatribe user's computer if he is granted permission to enter that user's network. In addition, users may remove other users from their network at will.

These security measures support the argument that Ladeau had a subjective expectation of privacy in his computer files. He controlled who accessed the files, and which files would be available to share with other users. Such security measures, however, do not establish that his expectation was objectively reasonable.

No matter how strictly Ladeau controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access. The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-744. That includes information turned over to parties who eventually reveal such information to the police. In *United States v. White*, the Supreme Court held that the law permits the "frustration of actual expectations of privacy by permitting authorities to use the testimony of those associates who for one reason or another have determined to turn to the police. . . ." 401 U.S. 745, 752 (1971). A person committing criminal activity who shares information with another person bears the risk that the other person will turn it over to the police. *Id.*; *see also Hoffa v. United States*, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

In this case, Ladeau bore the risk that any person who had access to his Gigatribe network would provide information to the police about illegal acts occurring on the network. As a

consequence, he also bore the risk that such a person would enable the police to access the network and download any files Ladeau made available for download. The RCMP was therefore allowed to use information provided by a third party to access Ladeau's Gigatribe network.[1] Once Ladeau turned over the information about how to access the network to a third party, his expectation of privacy in the network became objectively unreasonable. Because the files he claims were private were made available to anyone on the network, his expectation of privacy in those files was also objectively unreasonable. There was, accordingly, no violation of the Fourth Amendment in the search of Ladeau's computer.

B. Probable Cause

A "warrant application must demonstrate probable cause to believe that (1) a crime has been committed—the 'commission' element, and (2) enumerated evidence of the offense will be found at the place to be searched—the so-called 'nexus' element." *United States v. Ribeiro*, 397 F.3d 42, 48 (1st Cir. 2005) (quotation omitted). In reviewing the warrant, the Court must pay "great deference" to the magistrate's determination of probable cause and should not upset that determination unless the magistrate lacked a "substantial basis" for concluding that the search would uncover evidence of wrongdoing. *United States v. Santiago*, 389 F. Supp. 2d 124, 127 (D. Mass. 2005) (citing *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). There is no dispute that the LaForte affidavit established probable cause to believe that a crime had been committed; the Court, therefore, need only decide whether the affidavit established probable cause to believe that evidence of the crime would be found at defendant's home.

[1] The fact that the RCMP themselves accessed the network with the consent of the informant and downloaded the files does not require a different result. The RCMP could have easily instructed the informant to download certain files and then had the informant turn the files over to them.

Applying the nexus requirement requires "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit[,] . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. Given the wide variety of factual contexts in which the probable cause requirement applies, this is necessarily a fact-dependent inquiry. In essence, however, the nexus requirement is satisfied if a person of reasonable caution has reason to believe that evidence of a crime will be found at the place to be searched. *United States v. Rodrigue*, 560 F.3d 29, 32 (1st Cir. 2009).

Ladeau asserts two principal arguments as to why the affidavit in support of the search warrant failed to provide probable cause that evidence of a crime would be found at his home. First, Ladeau contends that evidence that he had digital child pornography does not provide probable cause to believe that such pornography would be found in other forms, such as hard copies, videotapes, books, or magazines. (Def. Mem. at 11). Using the same rationale, he contends that there was no probable cause to believe that there would be evidence of communication with websites providing child pornography or payment to such websites. He contends that instead of specific examples of these items, the warrant instead included a list of items to be seized during the search that "appear[ed] to be a boiler-plate list of items that the government hoped to find on the premises." *Id.*[2]

---

[2] The list of items to be seized was detailed in Attachment B of LaForte's Affidavit. The sections that Ladeau takes issue with read as follows:

> 2. Images of child pornography/minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, in any form, including digital and hard copy and including photographs, negatives, motion pictures, films, videos, books, and magazines, wherever it may be stored or found, including, but not limited to, computer(s), computer systems or electronic media, as well as compact disks and floppy disks; . . .
>
> 3. Records, including electronic, of the subscription to, communication with, and access to any

The government contends that it follows as a matter of common sense that if there is evidence that one form of child pornography is likely to be found at a particular location, there is also probable cause to believe that other forms of child pornography will be found there, as well. Moreover, the government contends, if there is evidence that the defendant obtained child pornography online and provided it to others, there is probable cause to believe evidence of other online activity related to child pornography exists.

The Court agrees that, under the circumstances presented here, the evidence that digital child pornography would be found at Ladeau's home provided probable cause that child pornography in other forms would also be found. Because child pornography can be produced in several different formats—and because it can be readily changed from one format to another (such as scanning a photograph to produce a digital image, or printing a digital image to photographic paper)—it makes little sense to require that specific evidence of each format be provided to a magistrate judge to support the issuance of a warrant that authorizes a seizure of child pornography in that particular form. Furthermore, the presence of child pornography in one format makes it probable that child pornography would also exist in a different format, given the ease of conversion between formats and relative unimportance of the format to the user's ability to view the image. For these purposes, therefore, there is no real distinction between child pornography in a digital format, an analog format, or a photographic format. Similarly, if the defendant obtained child pornography from an online provider, there was probable cause to

---

website or other Internet source offering images of child pornography; . . .

5. Credit card records reflecting payment for a subscription to any website offering images of child pornography.

believe that the defendant also sought to obtain child pornography from other online providers, whether for free or upon payment of a fee. The obtaining of images from the Gigatribe network was not a one-time or isolated event, and it is likely that the defendant at least sought child pornography from other sources, whether or not he obtained it.

Next, Ladeau argues that the information contained in LaForte's affidavit was stale. The evidence that Ladeau possessed child pornography was that the RCMP had downloaded it from Ladeau's computer in August 2008, eight months before LaForte applied for the warrant in April 2009. Ladeau contends that the delay between discovering his activity and obtaining the warrant was too great, and that by the time the warrant was obtained there was no longer probable cause to support it. Specifically, he argues that there was no evidence that Ladeau was a child pornography collector who was likely to retain a collection for an extended period of time. He also contends that the magistrate should have given minimal credit to the "untrained psychological conclusions rendered by the Affiant." Finally, he contends that because of the availability of child pornography on the Internet there is no longer a need for people interested in it to retain it for long periods of time. (Def. Mem. at 13).

The government contends that the eight-month delay between the discovery of Ladeau's activity and obtaining the warrant did not render the evidence stale. In support of its position it cites several cases in which courts have found that child pornography collectors and traders retain their collections for extensive periods of time. *See United States v. Ricciardelli*, 998 F.2d 8, 12, n. 4 (1st Cir. 1993) (finding that "exigent circumstances will rarely, if ever, be present in child pornography cases, as history teaches that collectors prefer not to dispose of their dross, typically retaining obscene materials for years"); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119

(1st Cir. 2008) (finding that evidence was not stale despite more than three-year gap between acquisition of evidence and acquisition of the warrant); *United States v. Lacy*, 119 F.3d 742, 745-746 (9th Cir. 1997) (finding that evidence was not stale despite ten-month delay between discovery of evidence and issuance of warrant); *United States v. Sherr*, 400 F. Supp. 2d 843, 847 (D. Md. 2005) (finding that evidence was not stale despite eight-month gap between defendant's receipt of child pornography and issuance of warrant).

In addition, the government contends that there was evidence in LaForte's affidavit other than possession of actual child pornography to suggest that Ladeau could be considered a collector. He had at least 171 files on his computer that were believed to contain child pornography. Not only did he possess these files, he also made them available to other people on his Gigatribe network. Moreover, the government contends, the videos downloaded from his computer contained hardcore videos depicting sadistic acts toward children. The affidavit also contained information about Ladeau's arrest for the molestation of a 12-year-old boy in 2008. Finally, LaForte's affidavit included a statement that, based on his training and experience, child pornography collectors retain their collections for long periods of time. Taking the evidence as a whole, the government contends, it is reasonable to conclude that Ladeau was a collector of child pornography and that the videos downloaded in August 2008 would still be on his computer when the warrant was issued. (Gov. Mem. at 10, n. 7).[3]

When evaluating a claim of staleness, a court must look at several different factors. The

[3] The government also argues that even if Ladeau had deleted the pornographic files from his computer, they might still be retrievable. This argument is based on the idea that it is difficult to complete erase all traces of electronic files. The Ninth Circuit noted this argument in *United States v. Hay*, 231, F.3d 630 (9th Cir. 2000). There may be some merit to this argument, but the Court does not reach the issue in this case.

determination is not simply a matter of "counting the number of days that have elapsed" between the discovery of the information and the issuance of the warrant. *Morales-Aldahondo*, 524 F.3d at 119. The court must also look at the nature of the information supporting the warrant, the nature and characteristics of the alleged crimes, and the likely endurance of the information. *Id*. The *Ricciardelli* and *Morales-Aldahondo* cases establish that it is reasonable to infer that in cases involving child pornography collectors a significant amount of time may elapse before the evidence is considered stale.

In *Hay*, the Ninth Circuit addressed the issue of staleness in the context of a child pornography case. In that case, a search warrant was issued based on information that the defendant had received child pornography from a distributor in Canada six months before the warrant was issued. *Hay*, 231 F.3d at 632-633. In support of its conclusion that the pornography would actually be found at Hay's apartment, the Court noted that Hay had an "extreme interest in young children," as evidenced by statements Hay had published on a website detailing his involvement in teaching and babysitting children. *Id*. at 634. Hay argued that there was no evidence that he had exhibited a pattern of receiving and keeping child pornography, and therefore no reason to believe he would still possess it six months after he received it. The court stated that there were other "good reasons" to believe the images would still be there, one of which was Hay's interest in children. *Id*. at 636. That fact, taken together with evidence that he had received child pornography from a known distributor of such pornography, provided support for the conclusion that pornography would be found on his computer six months after the images were transmitted to him. *Id*. at 634.

Here, considering the totality of the circumstances, there was probable cause to issue the

warrant. Ladeau not only possessed child pornography, but also shared that pornography with others. Furthermore, the hardcore nature of the videos suggests that Ladeau was not someone who dabbled lightly in child pornography or possessed the videos by accident. There was also evidence that he may have molested a 12-year-old boy, indicating a sexual interest in children. Finally, there was credible evidence that people who collect child pornography typically retain their collections for considerable amounts of time. The evidence was therefore not stale, and there was probable cause to issue the warrant.

C. Execution of Warrant

Rule 41 governs the issuance and execution of search warrants. It requires, among other things, warrants to be executed within a specific time—at the time, no longer than 10 days (not counting certain intermediate days). Fed. R. Crim. P. 41(e)(2)(A)(I).[4] In this case, agents executed the warrant and seized items on April 15, 2009. However, they did not complete their investigation of the contents of the computer and the other items seized until May 13, 2009.

Ladeau contends that the failure to comply with Rule 41 rendered the warrant null and void, leaving federal agents with no authority to conduct the search. The failure to follow the rule deprived Ladeau of his property, including private information and communications, and financial records. (Def. Mem. at 17).

The Fourth Amendment contains no time restrictions on the execution of warrants. However, a warrant may be invalidated if there is unreasonable delay in executing it. *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005). The First Circuit explained in *Syphers* that

[4] Rule 41 has since been amended and the time limit is now 14 days, without counting intermediate days. Fed. R. Crim. P. 41(e)(2)(A)(i)(2010).

the policy behind the time limit in Rule 41 is to ensure that probable cause continues to exist when a warrant is executed, and to ensure that it is the magistrate judge, not the executing officers, who make that determination. *Id*. In *United States v. Triumph Capital Group, Inc.*, the court found that Rule 41 does not apply to the forensic examination of evidence that has already been seized. 211 F.R.D. 31, 66 (D. Conn. 2002). Specifically, the court found that a computer search that took longer than the time period allowed by Rule 41 was not unreasonable. It found that "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution." *Id*. In *Syphers*, the First Circuit also noted the complexity involved with computer searches and the fact that courts have allowed extra time for their execution. *Syphers*, 426 F.3d at 469.

Here, even assuming a violation of Rule 41, any such violation was immaterial because the length of time it took to complete the examination of the seized evidence was reasonable. The warrant was executed within the time period allowed by Rule 41, but the examination of the computers and digital storage devices was not completed until about one month later. LaForte's affidavit indicated that examination of the computer equipment could be lengthy because of the tactics criminal defendants use to hide their incriminating digital files. Despite this warning to the issuing magistrate judge, Ladeau still contends that because the agents took longer than the 10 days allowed by law to examine the seized evidence, the magistrate judge could not determine whether probable cause continued to exist. There was no danger, however, that the probable cause to satisfy the warrant would be stale when the actual forensic examination took place. Once the computers and storage devices were seized, the probable cause was not going to change

because the contents of the computer equipment could not change. If there was a technical violation of Rule 41, it was immaterial and it did not render the warrant null and void.

III. Conclusion

The Court concludes that the remote download of the files from Ladeau's computer by the RCMP did not violate the Fourth Amendment. Furthermore, there was probable cause for the search; the evidence to support the warrant was not stale; and there was no violation of Rule 41 that requires suppression of the fruits of the search. For these reasons, defendant's motion to suppress is DENIED.

So Ordered.

/s/ F. Dennis Saylor
F. Dennis Saylor IV
United States District Judge

Dated: April 7, 2010